IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

KAJEET, INC.,	§	
	§	
Plaintiff,	§	Case No. 6:21-cv-389-ADA
	§	
v.	§	**JURY TRIAL DEMANDED**
	§	
TREND MICRO INC.,	§	
	§	
Defendant.	§	

DEFENDANT TREND MICRO INC.'S MOTION TO DISMISS UNDER FEDERAL RULE 12(B)(6) FOR FAILURE TO STATE A CLAIM

TABLE OF CONTENTS

I. INTRODUCTION 1

II. BACKGROUND 2

A. Kajeet Characterizes the '559 Patent Claims to Require a Policy Stored at the Server 3

B. The Infringement Allegations Are Unsupported 4

C. The Complaint's Allegations Concerning the Operation of the Accused Devices Are Contradicted by the Product Guide 6

1. Installation of the Trend Micro Security Software on a Device 7

2. Selection of the Parental Control Feature on the Device 7

III. LEGAL STANDARD 10

IV. ARGUMENT 11

A. Kajeet's Complaint Should Be Dismissed as Its Infringement Allegations Contradict the Attached Product Guide for the Accused Products 11

B. Kajeet's Complaint Must Be Dismissed with Prejudice as Granting Leave to Amend Is Futile And Kajeet Filed Its Deficient Complaint Knowing It Was Defective 15

C. A Broader Interpretation of the Claims Renders Them Invalid under 35 U.S.C. § 101 16

V. CONCLUSION 18

TABLE OF AUTHORITIES

Page(s)

Cases

Ashcroft v. Iqbal,
556 U.S. 662 (2009).....11, 13

Associated Builders, Inc. v. Alabama Power Co.,
505 F.2d 97 (5th Cir. 1974).....12

Bell Atlantic Corp. v. Twombly,
550 U.S. 544 (2007).....1, 10, 12

Bernal Lara v. Toro Bronco Corp.,
EP-15-CV-200-DB, 2016 WL 4401256 (W.D. Tex. Mar. 14, 2016).....11

Chapterhouse, LLC v. Shopify, Inc.,
2:18-CV-00300-JRG, 2018 WL 6981828 (E.D. Tex. Dec. 11, 2018).....11

Dorsey v. Portfolio Equities, Inc.,
540 F.3d 333 (5th Cir. 2008).....11

Dr. Adekunle C. Omoyosi, v. Texas Health & Human Services Commission,
4:20-CV-03315, 2021 WL 2689851 (S.D. Tex. June 14, 2021).....16

Ericsson, Inc. v. TCL Communication Technology Holdings, Ltd.,
955 F.3d 1317 (Fed. Cir. 2020).....17

Gharb v. Mitsubishi Elec. Automation, Inc.,
No. 10 C 07204, 2012 WL 1986435 (N.D. Ill. June 4, 2012).....15

Kajeet, Inc. v. Gryphon Online Safety, Inc.,
C.A. No. 19-2370 (MN), 2021 WL 780737 (D. Del. Mar. 1, 2021).....*passim*

Kajeet, Inc. v. Mosyle Corp.,
Case No. 1:21-cv-00006-MN (D. Del. April 8, 2021), Dkt. No. 21.....4

Kajeet, Inc. v. Qustodio, LLC,
Case No. 8:18-cv-01519-JAK-PLA (C.D. Cal. Nov. 1, 2019), Dkt. No. 140.....4, 13, 17

Limelight Networks, Inc. v. Akamai Techs., Inc.,
134 S. Ct. 2111 (2014).....12

Meetrix IP, LLC v. Cisco Sys., Inc.,
No. 1-18-CV-309-LY, 2018 WL 8261315 (W.D. Tex. Nov. 30, 2018).....11

O'Malley v. Brown Brothers Harriman & Co.,
2020 WL 1033658 (W.D. Tex. Mar. 3, 2020) (Pulliam, J.) 15

Qwikcash, LLC v. Blackhawk Network Holdings, Inc.,
2020 WL 6781566 (E.D. Tex. 2020) 12

Stockwell v. Kanan,
442 F. App'x 911 (5th Cir. 2011) 11, 12

Tenaha Licensing LLC v. TigerConnect, Inc.,
Civil Action No.19-1400-LPS-SRF (D. Del. Jan. 2, 2020) 16

Wright's Well Control Services, LLC v. Oceaneering Intl., Inc.,
CV 15-1720, 2017 WL 568781 (E.D. La. Feb. 13, 2017) 12

Statutes

35 U.S.C. § 101 ..... *passim*

35 U.S.C. §§ 271(a), (b), and (c) 5

Other Authorities

Rule 12(b)(6).....11

"Trend Micro Security 2021 for Windows Product Guide" 1

U.S. Patent No. 8,667,559..... *passim*

I. INTRODUCTION

Trend Micro Inc. ("Trend Micro") respectfully requests that this Court dismiss Kajeet Inc.'s ("Kajeet") Complaint for patent infringement with prejudice. The Complaint's sole claim for infringement of U.S. Patent No. 8,667,559 ("the '559 Patent") rests upon unfounded allegations that fail to state a claim that is plausible on its face for at least two reasons.

First, Kajeet skirts the well-accepted *Twombly*[1] pleading standard by failing to allege that the Accused Products operate such that they meet each and every limitation of any claim of the '559 Patent. Nor could it make such allegations in good faith. Over a month before Kajeet filed its Complaint, Kajeet had a similarly deficient complaint asserting infringement of the '559 Patent dismissed for failing to map the limitations of the patent claims to the accused products.[2] Despite that, Kajeet repeated the same mistakes here. Why? Because a good faith, limitation-by-limitation analysis would not support Kajeet's claim of infringement.

Second, Kajeet's Complaint must be dismissed as its unsupported allegations regarding the functionality of the Accused Products directly contradict the publicly available "Trend Micro Security 2021 for Windows Product Guide" ("Product Guide"), attached to the Complaint.[3] Kajeet emphasizes in the Complaint (as it has for years to save the '559 Patent from invalidity under 35 U.S.C. § 101) that the limitations of claim 27[4] "mandate that the decision applied to effect control over the computing device is ***based on a policy stored at a server remote from the***

[1] *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007).
[2] *Kajeet, Inc. v. Gryphon Online Safety, Inc.*, C.A. No. 19-2370 (MN), 2021 WL 780737 (D. Del. Mar. 1, 2021).
[3] The Product Guide is attached to the Complaint as Exhibit C.
[4] Claim 27 is the sole claim identified in the Complaint as infringed. Kajeet has previously treated claim 27 as representative of all asserted claims of the'559 patent. *Gryphon*, 2021 WL 780737, at *7 ("Plaintiff agreed today that the claims of the '559 Patent rise and fall together for purposes of this motion.").

computing device." (Dkt. No. 1 at ¶ 35) (emphasis added). Kajeet then attempts to assert, through bare bone allegations, that the Accused Products operate in this same manner. However, these allegations are expressly contradicted by the Product Guide. The Product Guide is unequivocal that the Accused Products' access management policies are stored locally on the managed device. It makes no mention of any remotely stored policies. Consequently, Kajeet cannot in good faith set out a plausible claim of infringement, and the Complaint should be dismissed with prejudice.

To the extent this Court allows Kajeet to proceed with its defective infringement allegations against the Accused Products, which would encompass a method where policies are stored and applied on the managed device itself, the '559 Patent claims fail the *Alice* test for patent-eligible subject matter. At least one court has found that Kajeet's claims are directed to an abstract idea and has only held off on summarily invalidating the claims because Kajeet has pled that remote storage of policies creates a unique "distributed architecture" that constitutes an inventive concept under step two of the *Alice* test. Stripped of that fig leaf, Kajeet's claims certainly do not claim patent-eligible subject matter, and for that reason, Kajeet's Complaint should be dismissed with prejudice.

II. BACKGROUND

On April 21, 2021, Kajeet filed its Complaint (Dkt. No. 1) alleging that Trend Micro has directly (*id.* ¶ 39) and indirectly (*id.* ¶¶ 40-41) infringed the '559 Patent by making and selling its Premium Security Suite, Maximum Security, Internet Security, and Mobile Security software products, as well as any others that include Trend Micro's parental control features ("Accused Products") (*id.* at ¶ 21).

A. Kajeet Characterizes the '559 Patent Claims to Require a Policy Stored at the Server

Kajeet alleges the Accused Products infringe at least independent claim 27 of the '559 Patent, reproduced below, which is directed to a method for managing a computing device through policies stored at a server – i.e., remote from the managed computing device:

> 27. A method for controlling a computing device configured to execute a function using a communication network managed by a service provider, the method comprising:
>
> sending to a server a request to communicate with a remote computing device over the communication network;
>
> receiving in real-time from the server a decision granting or denying the request, the decision being based on ***a policy stored at the server*** and configured by an administrator; and
>
> enforcing the decision by enabling a communication with the remote computing device over the communication network when the decision grants the request and by disabling the communication when the decision denies the request, the communication being enabled or disabled ***without storing the policy on the computing device***.

(*Id.*, Ex. A at 18:38-53) (emphases added).

The Complaint acknowledges that claim 27 requires "a decision [that] is received in real time from a server, with the decision 'being based on a policy stored at the server…,' and that 'the communication being enabled or disabled without storing the policy on the computing device.'" (*Id.* at ¶ 34). Thus, the Complaint concludes that "[t]hese limitations mandate that the decision applied to effect control over the computing device is ***based on a policy stored at a server remote from the computing device***." (*Id.* at ¶ 35) (emphasis added). Going further, the Complaint distinguishes the claimed method from prior art, which "was not premised on application of decisions ***based upon policies stored at the server level***." (*Id.* at ¶ 37) (emphasis added).

The Complaint's characterization of the '559 Patent in this case is consistent with Kajeet's prior admissions in other litigations involving the '559 Patent. To survive motions to dismiss under

35 U.S.C. § 101, Kajeet has repeatedly underscored to other courts that the claimed method requires that the policies be stored and applied remotely from the managed device. For example, Kajeet has argued, and successfully persuaded other courts, that:

- "[T]he parties cannot reasonably dispute the plain claim language that shows that the ***claimed policy and claimed enforcement step*** in Claim 27 of the '559 Patent ***occur remote from the computing device***." (*Kajeet, Inc. v. Qustodio, LLC*, Case No. 8:18-cv-01519-JAK-PLA (C.D. Cal. Nov. 1, 2019), Dkt. No. 140 at 13) (emphasis added) (Exhibit A);

- "With respect to Claim 27 of the '559 Patent, the plain claim language supports the conclusion that ***the claims are limited to circumstances where policies are stored remotely***." (*Id.* at 20) (emphasis added);

- "Plaintiff's position regarding the nature of the claims is premised on the assertion that each of the asserted claims requires, ***and there is a technological improvement created by, policies for managing computing devices that are stored separately from the computing devices***." (*Kajeet, Inc. v. Qustodio, LLC*, Case No. 8:18-cv-01519-JAK-PLA (C.D. Cal. Feb. 28, 2019), Dkt. No. 56 at 6) (emphasis added) (Exhibit B); and

- "Kajeet addressed these shortcomings [of the prior art] by storing usage policies remotely from the communication device(s)." (*Kajeet, Inc. v. Mosyle Corp.*, Case No. 1:21-cv-00006-MN (D. Del. April 8, 2021), Dkt. No. 21 at 4.) (emphasis added) (Exhibit C).

B. The Infringement Allegations Are Unsupported

The Complaint contains allegations concerning the operation of the Accused Products that lack any factual or evidentiary support. (Dkt. No. 1 at ¶¶ 21–26). While Kajeet attached "relevant excerpts" of the Product Guide (*id.* at 10, n. 3) to the Complaint in support of its infringement claim, it neglected to cite even once to it. Had Kajeet reviewed the Product Guide, it would have realized that its description of the Accused Products directly contradicts its unsupported allegations.[5]

[5] For completeness, the full version of the Product Guide is attached hereto as Exhibit D and references will be made to that version. The Complaint provided a website link to the full version

Kajeet's erroneous allegations concerning the Accused Products' storage of policies include:

- "[T]he Accused Products accommodate management of mobile communication devices accessing content over communication networks via application of remotely stored master policies set by administrators (e.g., parents)." (*Id.* at ¶ 21).

- "Execution of local agent software (client software) [that] effects control of the device via regular and/or scheduled sending of feature use requests ***to the Trend Micro servers for policy application***," or, in the alternative, "the local agent software effects control via regular installation and updates of use decisions ***based upon master policies stored on Trend Micro's servers*** (or derivatives thereof) via communication with the Trend Micro servers for on-device enforcement." (*Id.* at ¶ 23) (emphasis added).

- "Upon information and belief, the Accused Products effect feature management over devices connected to a communication network ***without storing the master policies on the devices, themselves or accessing the policies by the device***." (*Id.* at ¶ 26) (emphasis added).

The Complaint then recites bare bone allegations of direct infringement, induced infringement, and contributory infringement, respectively that essentially parrot the statutory language in 35 U.S.C. §§ 271(a), (b), and (c), respectively. (*Id.* at ¶¶ 39-41). Kajeet does not cite a single technical document or other information that illustrate that the Accused Products function the way the claims of the '559 Patent require.

As to direct infringement, for example, the Complaint accuses Trend Micro of "mak[ing], … us[ing], and sell[ing] the Accused Products which infringe at least claim 27 of the '559 Patent, among others, and [ ] us[ing] the Accused Products in a manner that meets every limitation of claim 27." (*Id.* at ¶ 39). Aside from this conclusory allegation, Kajeet fails to explain how the method practiced by any of the Accused Products meets each limitation of claim 27 (or any other claim) of the '559 Patent. Additionally, the Complaint's allegations of induced and contributory

---

of the Product Guide, and therefore is properly part of the record before the Court for purposes of this Motion. (Dkt. No. 1 at ¶ 27).

infringement are no more detailed about how third party use of the Accused Products lines up with each of the claim limitations. Kajeet conspicuously fails to substantiate these allegations by citing any particular statements in the Product Guide or any other factual information.

Kajeet was well aware of this deficiency over a month before it filed its Complaint in this case. On March 1, 2021, the District of Delaware dismissed its nearly-identical complaint against another defendant for infringement of the same patent. *Kajeet, Inc. v. Gryphon Online Safety, Inc.*, C.A. No. 19-2370 (MN), 2021 WL 780737, at *9, *16 (D. Del., Mar. 1, 2021) ("Gryphon's motion to dismiss as it relates to the *Iqbal / Twombly* issues is therefore granted . . . [and b]ecause Plaintiff has failed to adequately plead an underlying act of direct infringement, the claims of indirect infringement must also be dismissed."). Even with that court's clear guidance, Kajeet declined to remedy those deficiencies prior to bringing this lawsuit against Trend Micro.

C. The Complaint's Allegations Concerning the Operation of the Accused Devices Are Contradicted by the Product Guide

Notwithstanding any reference to it in the Complaint, the Product Guide describes in detail the operation of at least one Accused Product and demonstrates that it does not involve policies stored at a server level. (*See* Dkt. No. 1, Ex. C; Ex. D). To the contrary, the Product Guide illustrates that the policies used to manage the devices are found only ***on the devices themselves***. The Product Guide, titled "Trend Micro Security 2021 for Windows Product Guide," is meant to "provide[] help for analysts, reviewers, potential customers, and users who are evaluating, reviewing, or using the 2021 (v17) version of Trend Micro™ Antivirus+ Security, Trend Micro™ Internet Security, or Trend Micro™ Maximum Security on the Windows platform."[6] (Ex. D at 2).

[6] Additionally, Kajeet alleges in the Complaint that the Product Guide is an example of Trend Micro's other product guides, implying that the Accused Products share the same relevant operational features for purposes of its infringement allegations. (Dkt. No. 1 at ¶ 27).

The "Parental Control" feature is found only in the "Trend Micro Antivirus for Mac," "Trend Micro Internet Security" and "Trend Micro Maximum Security" versions. (*Id*. at 12).

1. Installation of the Trend Micro Security Software on a Device

The Product Guide begins by providing various avenues by which to install the application associated with the Accused Products directly on the computer or mobile device to be managed. (*Id.* at 16, 38, 181, and 183). For example, "Chapter 2: Installing and Activating Trend Micro Security" provides step-by-step instructions for downloading the software onto a device with a Windows 10 operating system and acknowledges that "each version of Trend Micro Security has a nearly identical installation and activation process." (*Id*. at 16-22). The Product Guide provides instructions for downloading the software onto the device (*id*. at 16-20) and installing the software onto the device by extracting the installer files and agreeing to the license agreement to complete the installation process (*id*. at 20-22).

The Product Guide also notes that certain versions allow for the protection of other devices. Once the additional devices are identified or selected, either manually or through a network scan, the Maximum Security software can then be downloaded onto that managed device for installation and setup. (*Id*. at 32, 34, 36). For example, once a device is identified through the network scan, the software is then downloaded and installed on that device: "Tap Install to install Trend Micro Security/Mobile Security ***on that device***. A screen appears, with options for downloading and installing it." (*Id*. at 34) (emphasis added). There is no discussion of any policies for managing the device being set, stored or applied remotely from the managed device.

2. Selection of the Parental Control Feature on the Device

The Parental Control feature is an optional feature that can be enabled *after* Trend Micro Security is installed and activated. (*Id*. at 29-32 (listing optional features that can be enabled to provide further protection for the computer)).

- **Parental Controls.** (For Internet Security and Maximum Security.) Click **Set Up Now** to set up **Parental Controls** to protect your children when they go online. A screen appears for you to **Select a Password** to protect your **Parental Controls** settings, so they can't be changed without your password. You then complete the process for tailoring protection for the specific child, with age-appropriate settings. See the Family: Parental Controls section in this guide to learn more.

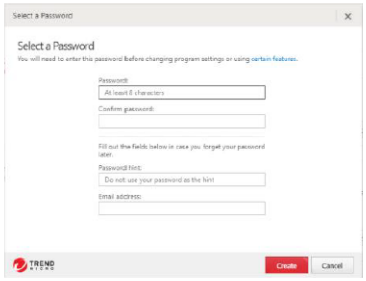
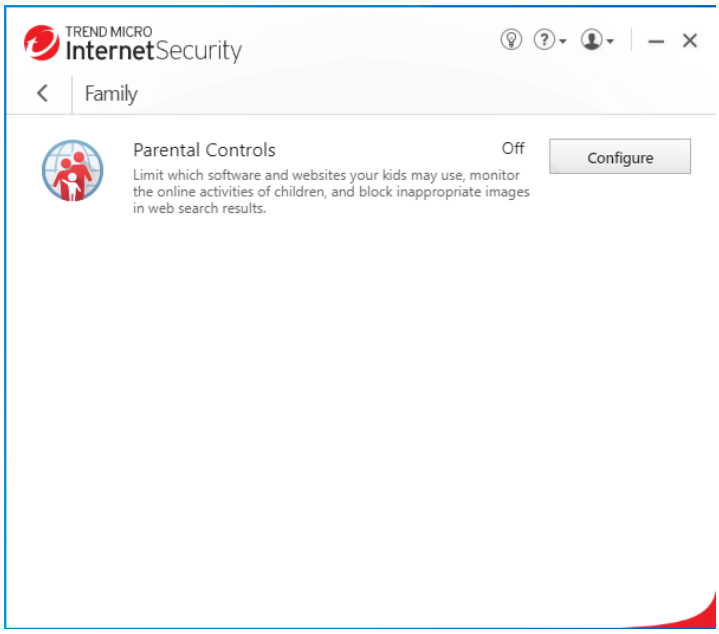


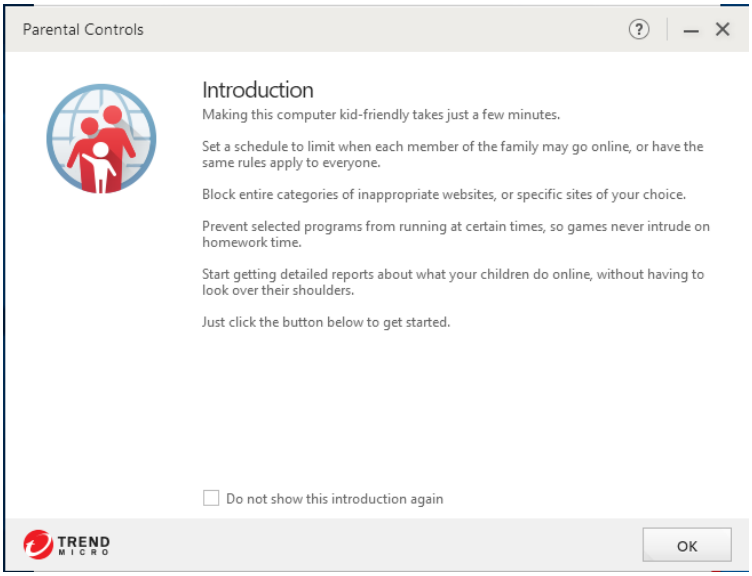
Figure 40. Select a Password - Begin to Set Up Parental Controls

(*Id*. at 31).

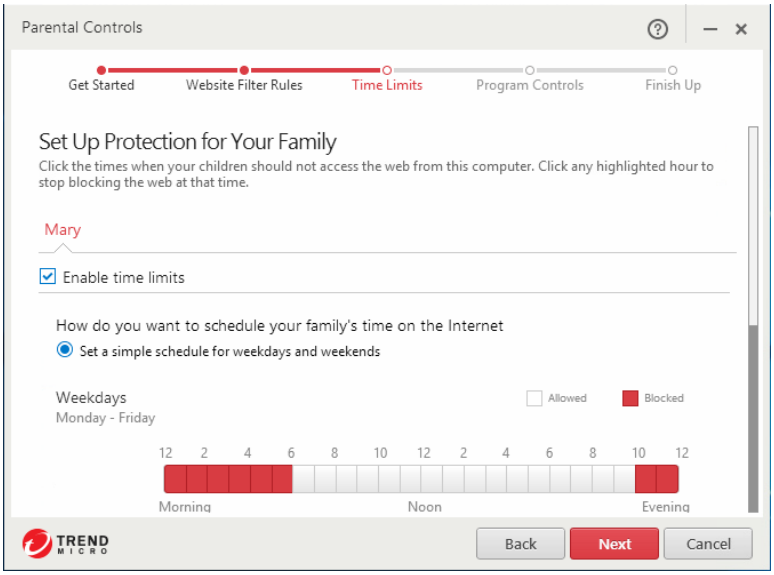
Once the Parental Control feature is enabled on the device, it is configured on the device directly. (*Id.* at 165 and 178 (directing an administrator to open the Trend Micro Security Console on the device to configure the feature)). These steps confirm that all aspects of the Accused Products reside, function, and are configured locally on a managed device, including the policies that relate to parental controls.



(*Id.*) The Product Guide makes clear that any Parental Control configurations restrict a child's access to certain activities or content ***on that particular device***. For example:



(*Id.* at 166) ("Making ***this computer*** kid-friendly takes just a few minutes.") (emphasis added).

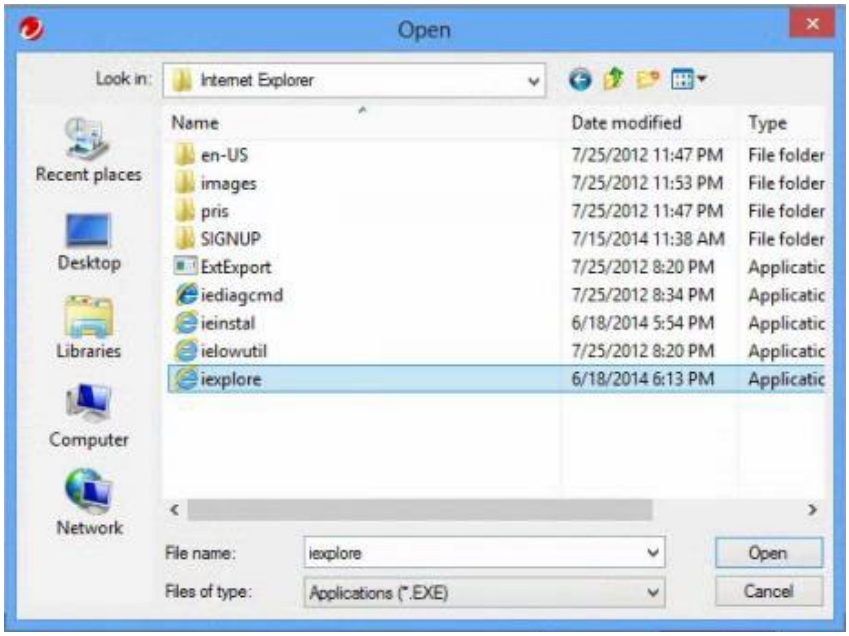


(*Id.* at 172) ("Click the times when your children should not access the web ***from this computer***.") (emphasis added). Additionally, just below this screen, the Product Guide provides:

> **Important note**: at the bottom of the screen you're asked **Do your children have their own Windows User Accounts for this computer?** If they don't, click the link on the question to create them, so your various settings can be assigned to the proper child. The **Parental Controls > Add Windows Account** screen appears.

(*Id.*) This passage further confirms that policies relating to parental controls are stored directly on the device as specific configurations are associated with a Windows User Account on the subject device. Moreover, if an individual does not have a Windows User Account, the Product Guide explains how to "[a]dd someone else ***to this PC***," wherein such addition is performed on that PC. (*Id.* at168) (emphasis added).

The Product Guide further illustrates how to internally (locally) restrict access to programs on a managed device. (*Id.* at 173) ("Select the program you want to control from the list, or click **Browse** to find it.").



(*Id.*)

III. LEGAL STANDARD

To survive a motion to dismiss, the allegations in Kajeet's Complaint must include "enough factual matter" that, when taken as true, "state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. 544 at 570. "This plausibility standard is met when 'the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the

misconduct alleged.'" *Meetrix IP, LLC v. Cisco Sys., Inc.*, No. 1-18-CV-309-LY, 2018 WL 8261315, at *1 (W.D. Tex. Nov. 30, 2018) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). Courts "are not bound to accept as true a legal conclusion couched as a factual allegation." *Iqbal*, U.S. at 678. Thus, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id*; *see also Chapterhouse, LLC v. Shopify, Inc*., 2:18-CV-00300-JRG, 2018 WL 6981828, at *2 (E.D. Tex. Dec. 11, 2018) (dismissing complaint where plaintiff failed to meet Iqbal/Twombly standard as asserted patent was directed to complicated software and plaintiff did not map claim elements to accused products).

In considering a Rule 12(b)(6) motion, a court ordinarily "may rely on only the complaint and its proper attachments." *Dorsey v. Portfolio Equities, Inc.*, 540 F.3d 333, 338 (5th Cir. 2008). While a court must "accept all well-pleaded facts of the complaint as true … [i]n case of a conflict between the allegations in a complaint and the exhibits attached to the complaint, the exhibits control." *Bernal Lara v. Toro Bronco Corp.*, EP-15-CV-200-DB, 2016 WL 4401256, at *3 (W.D. Tex. Mar. 14, 2016) (citing *Torch Liquidating Trust ex rel. Bridge Associates L.L.C. v. Stockstill*, 561 F.3d 377, 384 (5th Cir. 2009) (internal quotation marks and alterations omitted) (citing *In re Katrina Canal Breaches Litig*, 495 F.3d 191, 205 (5th Cir. 2007))); *Stockwell v. Kanan*, 442 Fed. Appx. 911, 913 (5th Cir. 2011) (citing *United States ex rel. Riley v. St. Luke's Episcopal Hosp.*, 355 F.3d 370, 377 (5th Cir. 2004), and *Simmons v. Peavy-Welsh Lumber Co.*, 113 F.2d 812, 813 (5th Cir. 1940)).

IV. ARGUMENT

A. Kajeet's Complaint Should Be Dismissed as Its Infringement Allegations Contradict the Attached Product Guide for the Accused Products

This Court should dismiss Kajeet's Complaint under Rule 12(b)(6) because Kajeet's allegations that the Accused Products infringe at least claim 27 of the '559 Patent directly

contradict the uncontroverted factual evidence provided in the Product Guide attached to the Complaint. By Kajeet's allegations in this Complaint, and repeated admissions in other cases, the claims of the '559 Patent all require that a managed device's access to content or applications be controlled according to policies that are ***stored and applied remotely from the managed device***. (*See supra* Sections II.A. and II.B). While Kajeet's Complaint summarily alleges that the Accused Products operate in that manner without support, the Product Guide clearly describes controlling a computing device using policies that are ***only stored locally on the device***, with no mention of remote policies. *See Limelight Networks, Inc. v. Akamai Techs., Inc.*, 134 S. Ct. 2111, 2117 (2014) ("A method patent claims a number of steps; under this Court's case law, the patent is not infringed unless all the steps are carried out."). In light of this glaring inconsistency, the Product Guide governs. *Stockwell v. Kanan*, 442 F. App'x 911, 913 (5th Cir. 2011) ("In case of a conflict between the allegations in a complaint and the exhibits attached to the complaint, the exhibits control."); *Associated Builders, Inc. v. Alabama Power Co.,* 505 F.2d 97, 100 (5th Cir. 1974) (dismissing complaint where allegations were contradicted by controlling attached exhibit). When the facts stated in the Product Guide are accepted over Kajeet's unsupported allegations to the contrary, Kajeet has failed to state a plausible claim for relief and its Complaint must be dismissed. *See, e.g*., *Qwikcash, LLC v. Blackhawk Network Holdings, Inc.*, 2020 WL 6781566, *3–*5 (E.D. Tex. 2020) (dismissing direct and indirect infringement claims and ruling that the patentee had pled itself out of court by making infringement allegations that were fatally inconsistent and rendered the claim of infringement to be implausible); *Wright's Well Control Services, LLC v. Oceaneering Intl., Inc.*, CV 15-1720, 2017 WL 568781, at *3 (E.D. La. Feb. 13, 2017) ("[T]he Court joins several other courts in holding that in order to properly plead direct infringement under *Twombly*

and *Iqbal*, a plaintiff must plausibly allege that a defendant directly infringes each limitation in at least one asserted claim.").

The plain language of claim 27, which Kajeet treats as representative, clearly requires that access management policies be stored on a server remote from the computing device. (Dkt. No. 1, Ex. A at 18:38-53). Claim 27 requires that the managed device "send[] to a server a request" and "receiv[e] in real-time from the server a decision granting or denying the request," where the decision is "based ***on a policy stored at the server***" and "the communication [is] enabled or disabled ***without storing the policy on the computing device***." (*Id.* at 18:44-45; 51-53) (emphasis added). Through admissions made in the Complaint and in other litigations, Kajeet concedes that the claims therefore require that the policies used to control the managed device are stored and applied remotely from that device. (*See, e.g.*, Dkt. No. 1 at ¶¶ 34, 35, and 36). For instance, Kajeet admits in the Complaint that "[t]hese limitations ***mandate*** that the decision applied to effect control over the computing device is based on a ***policy stored at a server remote from the computing device***." (*Id.* at ¶ 35; *see, e.g., id.* at ¶¶ 18, 19, 33, 36, and 37). Additionally, Kajeet asserted in *Qustodio* that "the parties cannot reasonably dispute the plain claim language that shows that ***the claimed policy and claimed enforcement step*** in Claim 27 of the '559 Patent ***occur remote from the computing device***." (Ex. A at 13).

To try to fit the square peg of the Accused Products into the round hole of this claim, Kajeet mistakenly alleges that "the Accused Products accommodate management of mobile communication devices accessing content over communication networks via application of ***remotely stored master policies*** set by administrators (e.g., parents)." (Dkt. No. 1 at ¶ 21) (emphasis added). The Product Guide, however, unequivocally undermines Kajeet's allegations. *See supra* Section II.C. The Accused Products control a computing device through policies that

are stored and configured locally on the computing device by setting the policies for a particular Windows User Accounts.

The Product Guide instructs an administrator, e.g., a parent, to create a child Windows User Account on a computer:

> 5. **Important note**: at the bottom of the screen you're asked **Do your children have their own Windows User Accounts for this computer?** If they don't, click the link on the question to create them, so your various settings can be assigned to the proper child. The **Parental Controls > Add Windows Account** screen appears.

(Ex. D at 166-167). Once the child Windows User Account is created (the Product Guide uses "Mary" as an example), the administrator then sets the rules for that account on the computer by selecting that account:

> 16. Back in the **Parental Controls > Add Windows Account** window, click the **Refresh** link if the new account is not showing. The **Mary** account now appears in the list.

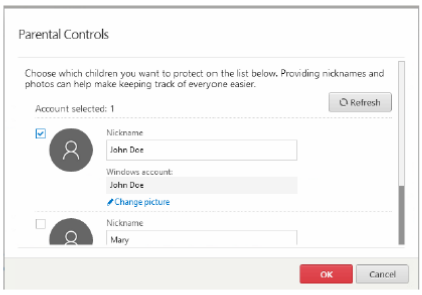


Figure 326. New Windows Account Listed

(*Id*. at 170). Next, it instructs the administrator to set the rules (or policies) for that account directly on the computer that is to be managed:

> 17. Uncheck the account you're logged on to, check the **Mary** account, and click **OK**. A popup appears, telling you "You have not set the rules for one or more users. Let's set it up now."

Figure 327. Set Up Rules Popup

(*Id*. at 172). To confirm that the rules for Mary's Windows User Account are set correctly, the Product Guide then instructs the administrator to switch to Mary's account on the computer and attempt to access prohibited content under Mary's account from the ***same*** computer. (*Id*. at 175-177).

In view of the above, the Product Guide unambiguously contradicts Kajeet's allegations that the Accused Products infringe based on managing computing devices through remotely stored policies. *See Gharb v. Mitsubishi Elec. Automation, Inc.*, No. 10 C 07204, 2012 WL 1986435, at *7-8 (N.D. Ill. June 4, 2012) (dismissing patent infringement claim pursuant to Rule 12(b)(6), where the complaint and its attached exhibits contradicted that patent was infringed). At a minimum, the Product Guide renders the allegations concerning the remote policy storage nothing more than mere speculation that cannot support a plausible claim of infringement. *O'Malley v. Brown Brothers Harriman & Co*., 2020 WL 1033658, at *4, *9 (W.D. Tex. Mar. 3, 2020) (Pulliam, J.) (dismissing complaint because allegations failed to "rise to a level above mere speculation.") Kajeet has thus failed to state a claim for direct infringement, induced infringement, and contributory infringement because the '559 Patent recites steps that differ from the functionality of the Accused Products as recited in the Product Guide.[7]

B. Kajeet's Complaint Must Be Dismissed with Prejudice as Granting Leave to Amend Is Futile And Kajeet Filed Its Deficient Complaint Knowing It Was Defective

Trend Micro requests that the motion be granted with prejudice because leave to amend would be futile. The Product Guide affirmatively shows that the Accused Product rely on local storage and application of policies, and the deficiencies in Kajeet's Complaint cannot be cured.

[7] *Gryphon*, 2021 WL 780737, at *16 ("Because Plaintiff has failed to adequately plead an underlying act of direct infringement, the claims of indirect infringement must also be dismissed.").

The operation of the Accused Products is fundamentally distinct from what claim 27 requires. No good faith amendment would remedy the implausibility of Kajeet's allegations. Therefore, the Court must grant Trend Micro's motion with prejudice. *See Tenaha Licensing LLC v. TigerConnect, Inc.*, Civil Action No.19-1400-LPS-SRF, at 19 (D. Del. Jan. 2, 2020) (granting Defendant's Motion to Dismiss with prejudice as the specification affirmatively contradicted Plaintiffs arguments regarding "specific improvements" and "any allegation of unconventionality in a subsequently amended complaint would not be plausible considering the contrary teachings of the specification at step one and 'inventive features' at step two.").

Dismissal with prejudice is also warranted in light of Kajeet's failure to address the deficiencies with the Complaint previously identified in the *Gryphon* decision, which placed Kajeet on notice at least two months prior to filing the present action. Instead of attempting to remedy the issues with its infringement claim, Kajeet simply parroted the same inadequate, conclusory allegations from the *Gryphon* case in its Complaint against Trend Micro. Such circumstances warrant dismissal with prejudice. *See Dr. Adekunle C. Omoyosi, v. Texas Health & Human Services Commission*, 4:20-CV-03315, 2021 WL 2689851, at *6 (S.D. Tex. June 14, 2021) ("[D]espite being put on notice of deficiencies in his Amended Complaint, Plaintiff's Second Amended Complaint fails to correct those deficiencies [and] … his claims should be dismissed with prejudice.")

C. A Broader Interpretation of the Claims Renders Them Invalid under 35 U.S.C. § 101

If Kajeet is permitted to allege that Trend Micro's Accused Products which store and apply policies locally fall within the scope of the '559 Patent claims, it cannot maintain its position that the asserted claims pass the *Alice* test for patent-eligible subject matter. Aside from being counter to what Kajeet alleges in the Complaint and its prior admissions, the broadening of the claim scope

would render the claims invalid under 35 U.S.C. § 101. In the context of defendants' motion to dismiss Kajeet's complaint, the District of Delaware previously found that under step one of the *Alice* framework, representative claim 27 of the '559 Patent is directed to the abstract idea of "controlling access to and the functionality of a device." *Gryphon*, 2021 WL 780737, at *6-*7; *see also Ericsson, Inc. v. TCL Communication Technology Holdings, Ltd*., 955 F.3d 1317 (Fed. Cir. 2020) ("Controlling access to resources is exactly the sort of process that 'can be performed in the human mind, or by a human using a pen and paper,' which we have repeatedly found unpatentable.").

However, at step two, the Delaware court concluded that the "complaints include[d] plausible factual allegations that the claimed invention improves upon the prior conventional systems by ***remotely storing policies for controlling access to the computing device***." *Gryphon*, 2021 WL 780737, at *6-*7 at *7 (emphasis added). Should Kajeet instead now argue, and the Court adopt for purposes of this motion, that the scope of claim 27 encompasses methods where policies are stored and applied locally on the managed computing device, then Kajeet cannot rely on its so called "distributed architecture" to argue that an inventive concept exists. For Kajeet to support a plausible claim of infringement, it must allege infringement of a method as described in Product Guide – i.e., one that involves a decision based on a policy stored that is stored on the computing device. Under a claim interpretation that encompasses the application of policies that reside on the device, the scope of the claims are then akin to those of the related patents that were found to be invalid under § 101 by the Central District of California in *Qustodio*. (Exhibit A at 19) ("As noted, the claim construction determined that remote policy storage is not a required limitation of Claim 1 of the '371 Patent or Claim 1 of the '612 Patent. Therefore, Plaintiff's stated basis for patent eligibility at *Alice* Step Two in which it refers to the particular arrangement of

claim elements to create a 'distributed architecture,' is again without force."). In response to an improper broadening of the claims, Trend Micro respectfully requests the Court to find the claims invalid under § 101 or – at a minimum – invite Trend Micro to bring a motion to dismiss seeking the same.

V. CONCLUSION

Trend Micro respectfully requests that Plaintiff's Complaint be dismissed with prejudice for the foregoing reasons.

Respectfully Submitted,

/s/ Katherine P. Chiarello

Katherine P. Chiarello
Texas State Bar No. 24006994
katherine@wittliffcutter.com

WITTLIFF | CUTTER, PLLC
1209 Nueces Street
Austin, Texas 78701
(512) 649.2434 office
(512) 960.4869 facsimile

Charanjit Brahma
(pro hac vice forthcoming pending)
Benesch Friedlander Coplan & Aronoff LLP
One Market Street, Spear Tower
36th Floor
San Francisco, CA 94105
(628) 600.2241 office
(628) 221.5828 facsimile
CBrahma@beneschlaw.com

Manish Mehta
(pro hac vice forthcoming)
Benesch Friedlander Coplan & Aronoff LLP
71 South Wacker Drive, Suite 1600
Chicago, IL 60606

(312) 212.4953 office
(628) 221.5828 facsimile
MMehta@beneschlaw.com

Attorneys for Defendant Trend Micro Incorporated

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure and Local Rule CV-5, I hereby certify that, on July 5, 2021, all counsel of record who have appeared in this case are being served with a copy of the foregoing via the Court's CM/ECF system.

/s/ Katherine P. Chiarello
Katherine P. Chiarello